(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 810 463 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
16.01.2019 Bulletin 2019/03

(21) Application number: **13702958.3**

(22) Date of filing: **28.01.2013**

(51) Int Cl.:
H04W 12/04 *(2009.01)* ***H04W 36/00*** *(2009.01)*

(86) International application number:
PCT/EP2013/051550

(87) International publication number:
WO 2013/113647 (08.08.2013 Gazette 2013/32)

(54) **CALL HANDOVER BETWEEN CELLULAR COMMUNICATION SYSTEM NODES THAT SUPPORT DIFFERENT SECURITY CONTEXTS**

RUFWEITERLEITUNG ZWISCHEN MOBILTELEFONKOMMUNIKATIONSSYSTEMKNOTEN ZUR UNTERSTÜTZUNG VERSCHIEDENER SICHERHEITSKONTEXTE

TRANSFERT D'APPEL ENTRE DES NOEUDS DE SYSTÈME DE COMMUNICATION CELLULAIRE QUI PRENNENT EN CHARGE DES CONTEXTES DE SÉCURITÉ DIFFÉRENTS

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

(30) Priority: **30.01.2012 US 201261592126 P**
15.11.2012 US 201213677451

(43) Date of publication of application:
10.12.2014 Bulletin 2014/50

(73) Proprietor: **Telefonaktiebolaget LM Ericsson (publ)**
164 83 Stockholm (SE)

(72) Inventors:
- **NORRMAN, Karl**
  S-116 28 Stockholm (SE)
- **WIFVESSON, Monika**
  S-226 52 Lund (SE)

(74) Representative: **Ericsson Patent Development**
Torshamnsgatan 21-23
164 80 Stockholm (SE)

(56) References cited:
EP-A2- 1 926 281

- **"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture (Release 11)", 3GPP STANDARD; 3GPP TS 33.102, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE, vol. SA WG3, no. V11.0.0, 26 September 2011 (2011-09-26), pages 1-71, XP050554024, [retrieved on 2011-09-26]**
- **"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture (Release 10)", 3GPP STANDARD; 3GPP TS 33.401, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE, vol. SA WG3, no. V10.1.1, 23 June 2011 (2011-06-23), pages 1-115, XP050553490, [retrieved on 2011-06-23]**

Printed by Jouve, 75001 PARIS (FR)

(Cont. next page)

- **"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Release 10)", 3GPP STANDARD; 3GPP TS 23.401, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE, vol. SA WG2, no. V10.5.0, 24 August 2011 (2011-08-24), pages 1-282, XP050553747, [retrieved on 2011-08-24] cited in the application**

Description

BACKGROUND

[0001] The present invention relates to cellular communication systems, and more particularly to the handover of calls between cellular communication systems that support different security contexts.

[0002] Cellular communication systems typically comprise a land-based network that provides wireless coverage to mobile terminals that can continue to receive service while moving around within the network's coverage area. The term "cellular" derives from the fact that the entire coverage area is divided up into so-called "cells", each of which is typically served by a particular radio transceiver station (or equivalent) associated with the land-based network. Such transceiver stations are often generically referred to as "base stations", even when particular communication standards setting bodies apply different terminology (e.g., "NodeB" in WCDMA, and "eNodeB" in LTE) for the purpose of very precisely pointing out the distinctive capabilities and architectures of their version of the base station. As the mobile device moves from one cell to another, the network hands over responsibility for serving the mobile device from the presently-serving cell to the "new" cell. In this way, the user of the mobile device experiences continuity of service without having to reestablish a connection to the network. Handovers are controlled by a system-defined cell reselection mechanism. FIG. 1 illustrates a cellular communication system providing a system coverage area 101 by means of a plurality of cells 103.

[0003] As new communication systems come into existence, they bring with them new features, capabilities, and ways of handling calls. The mobile communication equipment (hereinafter referred to as "User Equipment", or "UE") must operate in a way that is compatible with the system with which it is expected to communicate. In order to provide the most flexibility with respect to usage, UEs are often designed to be compatible with more than one system. In one respect, this enables a user to continue using the UE as it is carried from a geographical area covered by one type of communication system into another area, served by a different type of communication system.

[0004] Having multi-mode capability is also useful because newer systems are often rolled out piecemeal, so that even if a user stays within the geographical confines of one operator's system, the UE may find itself at times served by older equipment, and at other times served by newer equipment. This situation is illustrated in FIG. 2, which depicts a portion of a cellular communication system in which a UE 201 is presently being served within a first cell 203 that is supported by equipment 205 that conforms to an older communications standard (e.g., one of the 2G - e.g., GERAN - or 3G - e.g., UTRAN - standards). In this example, the UE 201 is in the vicinity of a second (neighboring) cell 207 that is supported by equipment 209 that conforms to a newer communication standard (e.g., a 4G specification, such as E-UTRAN which is also known as "Long Term Evolution" or "LTE"). If the user is engaged in a call at the time that a handover should be performed from the older equipment 205 to the newer equipment 209 it would be desirable to be able to handover the call in a graceful way that minimizes the call's disruption.

[0005] However, since older communication systems are not designed with the knowledge of what information will be required to support a handover to newer equipment, designers have been faced with the problem of how best to enable such handovers to take place (i.e., how to supply the new equipment with information that puts it in the best position to pick up support for the ongoing call that is presently served by older equipment). Solutions to this problem, involving methods, apparatuses, and/or software are therefore desired.

SUMMARY

[0006] The invention is defined in the independent claims. Additional features of the invention are provided in the dependent claims. The embodiments disclosed in the following description which are not covered by the appended claims are considered as not being part of the present invention.

[0007] In accordance with one aspect of the present invention, the foregoing and other objects are achieved in, for example, methods and apparatuses for operating a target packet switched node to generate a security context for a client in a cellular communication system as part of a handover of a circuit switched connection from a source circuit switched node to the target packet switched node, wherein the target packet switched node comprises processing circuitry. Such operation includes the target packet switched node receiving at least one cryptographic key from a source circuit switched node, and receiving identities of security algorithms supported by the client from a source packet switched node. The at least one cryptographic key and the identities are used to generate the security context for the client.

[0008] For example, the target packet switched node can be an MME, the source circuit switched node can be an MSC and the source packet switched node can be an SGSN. In some alternative embodiments, the source circuit switched node is a first SGSN, the source circuit switched node is an MSC and the source packet switched node is a second SGSN.

[0009] In some embodiments, operation further comprises the target packet switched node receiving one or more authentication vectors from the source circuit switched node. The authentication vectors received from the source circuit switched node are then discarded.

[0010] In some embodiments in which the target packet switched node is an SGSN, operation comprises using one or more of the at least one cryptographic key to protect traffic between a fourth node and the client.

[0011] In some embodiments in which the target packet switched node is an MME, operation includes deriving a key for an Access Security Management Entity (K ASME) from one or more of the at least one cryptographic key.

[0012] In some embodiments, operation includes receiving, from the source packet switched node, packet switched encryption keys for use in a packet switched connection, and discarding the packet switched encryption keys.

[0013] In some embodiments, operation includes receiving at least one authentication vector from the source packet switched node and storing the received at least one authentication vector.

[0014] In some embodiments, operation includes receiving additional information from the source packet switched node, and in some of these embodiments using the at least one cryptographic key and the identities to generate the security context for the client includes using the at least one cryptographic key and the identities and the additional information to generate the security context for the client.

[0015] Some embodiments cover operation in both the target packet switched and source circuit switched nodes, such that the source circuit switched node generates at least one new cryptographic key from at least one existing key associated with the client and a nonce generated by the source circuit switched node, and communicates the at least one new cryptographic key to the target packet switched node. The target packet switched node then receives identities of security algorithms supported by the client from a source packet switched node and uses the at least one cryptographic key and the identities to generate the security context for the client.

BRIEF DESCRIPTION OF THE DRAWINGS

[0016]

FIG. 1 illustrates a cellular communication system providing a system coverage area by means of a plurality of cells.

FIG. 2 depicts a portion of a cellular communication system in which a UE is presently being served within a first cell that is supported by equipment that conforms to an older communications standard (e.g., one of the 2G or 3G standards) and that should be handed over to a second cell that is supported by equipment that conforms to a newer communications standard.

FIG. 3 depicts aspects of signaling involved in the handover of a call from source UTRAN or GERAN supporting equipment operating in the circuit switched domain to target UTRAN/GERAN supporting equipment operating in the PS domain.

FIG. 4 depicts aspects of signaling involved in the handover of a call from source UTRAN or GERAN supporting equipment operating in the CS domain to target E-UTRAN (i.e., 4G equipment) supporting equipment operating in the PS domain.

FIG. 5 is, in one respect, a flow chart of steps/processes performed by a target PS node in accordance with some but not necessarily all exemplary embodiments of a handover mechanism consistent with the invention.

FIG. 6 is a signaling diagram of aspects of one embodiment of handover signaling and steps consistent with the invention.

FIG. 7 is a signaling diagram of an alternative embodiment of handover signaling and steps consistent with the invention.

FIG. 8 is a block diagram of a target node (e.g., SGSN/MME) that operates in the PS domain.

DETAILED DESCRIPTION

[0017] The various features of the invention will now be described with reference to the figures, in which like parts are identified with the same reference characters.

[0018] The various aspects of the invention will now be described in greater detail in connection with a number of exemplary embodiments. To facilitate an understanding of the invention, many aspects of the invention are described in terms of sequences of actions to be performed by elements of a computer system or other hardware capable of executing programmed instructions. It will be recognized that in each of the embodiments, the various actions could be performed by specialized circuits (e.g., analog and/or discrete logic gates interconnected to perform a specialized function), by one or more processors programmed with a suitable set of instructions, or by a combination of both. The term "circuitry configured to" perform one or more described actions is used herein to refer to any such embodiment (i.e., one or more specialized circuits and/or one or more programmed processors). Moreover, the invention can additionally be considered to be embodied entirely within any form of computer readable carrier, such as solid-state memory, magnetic disk, or optical disk containing an appropriate set of computer instructions that would cause a processor to carry out the techniques described herein. Thus, the various aspects of the invention may be embodied in many different forms, and all such forms are contemplated to be within the scope of the invention. For each of the various aspects of the invention,

any such form of embodiments as described above may be referred to herein as "logic configured to" perform a described action, or alternatively as "logic that" performs a described action.

[0019] In the following disclosure, a number of abbreviations are used for the sake of conciseness and since the abbreviations are widely used in the field. Therefore, the following abbreviations and their meanings are presented with the understanding that each is standard terminology that would be readily understood by a person of ordinary skill in the art:

- 3GPP (3rd Generation Partnership Project)
- 3GPP TSG SA WG3 (3rd Generation Partnership Project Technical Specification Group System Architecture Work Group 3)
- AKA (Authentication and Key Agreement)
- AMF (Authentication management field)
- AS (Access Stratum)
- BSC (Base Station Controller)
- BSS (Base Station Subsystem)
- CK (Ciphering Key)
- CKSN (Ciphering Key Sequence Number)
- CR (Change Request)
- CS (Circuit Switched)
- eNB (eNodeB)
- E-UTRAN (Evolved-Universal Terrestrial Radio Access Network)
- EPS (Evolved Packet System)
- FC (Function Code)
- FFS (For Further Study)
- GERAN (GSM/EDGE Radio Access Network)
- HLR (Home Location Register)
- HO (Handover)
- HSPA (High Speed Packet Access)
- HSS (Home Subscriber Server)
- IE (Information Element)
- IK (Integrity Key)
- IMS (IP Multimedia Subsystem)
- IMSI (International Mobile Subscriber Identity)
- IRAT (Inter Radio Access Technology)
- ISDN (Integrated Services Digital Network)
- K_{ASME} (Key Access Security Management Entity)
- KDF (Key Derivation Function)
- KSI (Key Set Identifier)
- LA (Location Area)
- LTE (Long Time Evolution)
- ME (Mobile Equipment)
- MSC (Mobile Switching Centre)
- MSISDN (Mobile Subscriber ISDN)
- MM (Mobility Management)
- MME (Mobility Management Entity)
- MS (Mobile Station)
- NAS (Non-Access Stratum)
- NB (Node B)
- NONCE ("Number Used Once" - A (pseudo) randomly generated string of bits)
- PLMN (Public Land Mobile Network)
- PS (Packet Switched)
- PRNG (Pseudo Random Number Generator)
- RAT (Radio Access Technology)
- RNC (Radio Network Controller)
- RRC (Radio Resource Control)
- SA (System Architecture)
- SGSN (Serving GPRS Support Node)
- SGW (Signaling Gateway)
- SIM (Subscriber Identity Module)

- SRNC (Serving RNC)
- SRVCC (Single Radio Voice Call Continuity)
- SQN (Sequence Number)
- UE (User Equipment)
- USIM (Universal Subscriber Identity Module)
- UTRAN (Universal Terrestrial Radio Access Network)
- UMTS (Universal Mobile Telecommunication System)
- UP (User Plane)

[0020] As mentioned in the Background section of this disclosure, incompatibilities between different types of cellular communication equipment present impediments to achieving high quality handovers of calls from one type of equipment to another type. As an example, consider the problems that can arise with respect to the security context when newer, so-called "4G" equipment is to pick up responsibility for a call that is presently being served by older "2G" or "3G" equipment. Dual/multi-mode UEs that are designed to operate in 2G/3G equipment as well as in newer 4G equipment will likely have security capabilities that are specific to the 4G equipment. Therefore, the 4G network node to which a call is to be handed over should receive information indicating what the UE's 4G security parameters (e.g., keys, selected and supported ciphering algorithms, etc.) are. But consider what happens during a conventional handover from 2G/3G equipment to 4G equipment:

Any 2G/3G call (which can operate in either circuit switched - CS - or packet switched - PS - mode) that is to be handed over to 4G equipment (which operates exclusively in a PS mode) must at least be attached to an SGSN (PS equipment) even if the call is being handled by means of a connection to an MSC (CS equipment). When the UE attaches to the network in the packet switched domain it provides the SGSN with the so-called "UE Network capabilities", which includes the security algorithms that the terminal supports in E-UTRAN. Clause 6.14 of 3GPP TS 23.060 V10.6.0 (2011-12) specifies that the "radio access classmark" contains the "UE Network capability." The "UE Network capability" contains the E-UTRAN security algorithms supported by the UE. In particular, clause 6.14.1 of 3GPP TS 23.060 states that the UE (referred to in the specification as "MS", "Mobile Station" for historical reasons) sends the radio access capability to the network. The interested reader can refer to 3GPP TS 23.060 for more information about this aspect.

[0021] Looking now at the circuit switched domain, the UE does not provide the "UE Network capability" to the network (in this case, the MSC), but instead only provides its 2G/3G (UTAN/GERAN) related capabilities. This can be seen from the Location Update Request message definition that is found in clause 9.2.15 of 3GPP TS 24.008 V10.5.0 (2011-12). The Location Update Request message is used to perform the attach.

[0022] The Packet Switched Inter RAT handover from UTRAN (3G) to E-UTRAN (4G) is described in clause 5.5.2.2 of 3GPP TS 23.401 V10.6.0 (2011-12). Of particular interest is step 3 (Forward relocation request) shown in the specification as Figure 5.5.2.2.2-1. The security parameters (e.g., keys, selected and supported ciphering algorithms, etc.) are included in the MM Context. In particular, the MM context contains security related information, such as UE Network capabilities and used UMTS integrity and ciphering algorithms(s) as well as keys, as described in clause 5.7.2 (Information Storage for MME). The UE Network capabilities includes the E-UTRAN security capabilities, which include for example the identities of the LTE encryption and integrity algorithms the UE supports (these algorithm identifiers are called EPS encryption algorithms and EPS integrity protection algorithms in the LTE security specification TS 33.401).

[0023] The Packet Switched Inter RAT handover from GERAN to E-UTRAN is described in clause 5.5.2.4 of 3GPP TS 23.401.

[0024] The principle of having the source node (SGSN for the PS domain) forward the UE Network capabilities to the target node is exactly the same as the specified handover procedure when the call originates in the CS domain. However, in the CS domain the source node is an MSC which, as mentioned above, does not have the UE's E-UTRAN security capabilities. (Indeed, in the CS domain there is no need for the MSC to have such information because the target node is also an MSC.) Consequently, conventional handovers do not provide any mechanism for supplying this information to the target node (MME in E-UTRAN).

[0025] This situation is illustrated in FIG. 3, which depicts aspects of signaling involved in the handover of a call from source UTRAN or GERAN supporting equipment operating in the CS domain to target UTRAN supporting equipment operating in the PS domain. The illustrated components that participate in this signaling are a UE 301, a source BSC/RNC 303, a target RNC 305, an MSC server 307, a source SGSN/MME 309, and a target SGSN 311.

[0026] Initially, the UE 301 is engaged in a CS call, supported by the various source UTRAN or GERAN equipment. In response to a decision being made to perform the CS (UTRAN or GERAN) to PS (UTRAN) handover, in step 1 the source BSC/RNC 303 sends a "HO required" message to the MSC server 307.

[0027] The MSC server 307 then generates (step 313) a $NONCE_{MSC}$, and uses this to generate a cryptographic key in accordance with:

$$CK'_{PS} \parallel IK'_{PS} = KDF(CK_{CS}, IK_{CS}, NONCE_{MSC}),$$

where the symbol "‖" represents a concatenation function.

[0028] In step 2, the MSC server 307 communicates a "CS to PS HO request" to the target SGSN 311, and includes the generated cryptographic key ($CK'_{PS} \parallel IK'_{PS}$) in this message.

[0029] In response, in step 3 the target SGSN 311 sends a "Context request" to the source SGSN/MME 309 for the purpose of requesting context information for the UE 301. (Dashed lines used here and in other representations of signaling represent an optional step.) The SGSN/MME 309 then sends a "Context response" (including the requested information) back to the target SGSN 311 (step 4).

[0030] If the target SGSN 311 received a GPRS Kc' and a $CKSN'_{PS}$ from the MSC server 307 enhanced for SRVCC, then the target SGSN 311 computes (step 315) CK'_{PS} and IK'_{PS} from the GPRS Kc'. The target SGSN 311 associates the CK'_{PS} and IK'_{PS} with KSI'_{PS}, which is set equal to $CKSN'_{PS}$ received from the source MSC server 307 enhanced for SRVCC.

[0031] The target SGSN 311 then sends the CK'_{PS}, IK'_{PS} to the target RNC 305 (step 5). In response, the target RNC 305 sends an Allocate resources response (step 6).

[0032] In step 7, the target SGSN 311 sends a CS to PS HO Response message to the source MSC server 307.

[0033] In step 8, the MSC server 307 sends a CS to PS HO Response to the source BSC/RNC 303. This CS to PS HO Response includes, among other things, the $NONCE_{MSC}$.

[0034] In step 9, the source BSC/RNC 303 sends a CS to PS HO command to the UE 301. This command includes, among other things, the $NONCE_{MSC}$. The UE 301 uses the received $NONCE_{MSC}$ to derive CK'_{PS} and using key derivation formulas specified by the applicable standard (step 317).

[0035] In step 10, the UE 301 returns a CS to PS HO Confirmation to the target RNC 305. The CK'_{PS} AND IK'_{PS} become the active key set both in the UE 301 and in the target RNC 305.

[0036] An alternative illustration of the same type of situation is illustrated in FIG. 4, which depicts aspects of signaling involved in the handover of a call from source UTRAN or GERAN supporting equipment operating in the CS domain to target E-UTRAN (i.e., 4G equipment) supporting equipment operating in the PS domain. The illustrated components that participate in this signaling are a UE 401, a source BSC/RNC 403, a target eNB 405, an MSC server 407, a source SGSN/MME 409, and a target MME 411.

[0037] Initially, the UE 401 is engaged in a CS call, supported by the various source UTRAN or GERAN equipment. In response to a decision being made to perform the CS (UTRAN or GERAN) to PS (E-UTRAN) handover, in step 1' the source BSC/RNC 403 sends a "HO required" message to the MSC server 407.

[0038] The MSC server 407 then generates (step 413) a $NONCE_{MSC}$, and uses this to generate a cryptographic key in accordance with:

$$CK'_{PS} \parallel IK'_{PS} = KDF(CK_{CS}, IK_{CS}, NONCE_{MSC}),$$

where the symbol "‖" represents a concatenation function.

[0039] In step 2', the MSC server 407 communicates a "CS to PS HO request" to the target MME 411, and includes the generated cryptographic key ($CK'_{PS} \parallel IK'_{PS}$) in this message.

[0040] In response, in step 3' the target MME 411 sends a "Context request" to the source SGSN/MME 409 for the purpose of requesting context information for the UE 401. The SGSN/MME 409 then sends a "Context response" (including the requested information) back to the target MME 411 (step 4').

[0041] In step 415, the target MME 411 creates a mapped EPS security context by setting the K'_{ASME} of the mapped EPS security context equal to the concatenation $CK'_{PS} \parallel IK'_{PS}$, where the CK'_{PS} and were received in the CS to PS handover request (see step 2'). The target MME 411 further associates the K'_{ASME} with a KSI_{SGSN}. The value of the KSI_{SGSN} is the same as the value of the KSI'_{PS} received in the CS to PS handover request.

[0042] Also as part of step 415, the target MME 411 derives K_{eNB} by applying the KDF as defined in the applicable standard, using the mapped key K'_{ASME} and 2^{32}-1 as the value of the uplink NAS COUNT parameter. The uplink and downlink NAS COUNT values for the mapped EPS security context are set to start value (i.e., 0) in the target MME 411.

[0043] The target MME 411 then sends the K_{eNB} and NAS parameters to the target eNB 405 (step 5'). In response, the target eNB 405 sends an Allocate resources response (step 6').

[0044] In step 7', the target MME 411 sends a CS to PS HO Response message to the source MSC server 407.

[0045] In step 8', the MSC server 407 sends a CS to PS HO Response to the source BSC/RNC 403. This CS to PS HO Response includes, among other things, the $NONCE_{MSC}$.

[0046] In step 9', the source BSC/RNC 403 sends a CS to PS HO command to the UE 401. This command includes,

among other things, the $NONCE_{MSC}$. The UE 401 uses the received $NONCE_{MSC}$ to derive K'_{ASME}, associate it with KSI_{SGSN} received in the NAS Security Transparent Container IE and derive NAS keys and K_{eNB} following the same key derivations as the MSC server 407 and target MME 411 performed in steps 2', 3' and 4' (step 417), all as specified by the applicable standard.

[0047] In step 10', the UE 401 returns a CS to PS HO Confirmation to the target eNB 405. The mapped EPS security context established as above becomes the current EPS security context at AS.

[0048] A new handover mechanism addresses the problems with the conventional techniques. Aspects of this new handover mechanism are depicted in FIG. 5, which in one respect is a flow chart of steps/processes performed by a target PS node (e.g., a Target SGSN or Target MME) in accordance with some but not necessarily all exemplary embodiments of the invention. In another respect, FIG. 5 can be considered to depict exemplary means 500 comprising the various illustrated circuitry (e.g., hard-wired and/or suitably programmed processor) configured to perform the described functions.

[0049] For ease of terminology, the target PS node can, in the context of this processing, be considered a "first node" that generates a security context for a client in a cellular communication system. In one aspect, the first node receives at least one cryptographic key from a second node (step 501). The second node can be a source CS node such as an MSC.

[0050] The first node solicits from a third node (e.g., a source SGSN), and in response receives, identities of security algorithms supported by the client (step 503). In some but not necessarily all embodiments, the first node may also receive other information such as one or more authentication vectors and/or cryptographic key(s).

[0051] The first node then uses the at least one cryptographic key received from the second node and the security algorithm identities to generate the security context for the client (step 505). In some but not necessarily all embodiments, authentication vectors received from the second node may be used as well.

[0052] At this, point, the first node has generated the security context for the client. In some but not necessarily all embodiments, the first node may perform any one or combination of additional functions, such as but not limited to:

- discarding additional information received from the second and/or third nodes (e.g., authentication vectors received from the second and/or third nodes, cryptographic key(s) received from the third node)
- using (e.g., if the target PS node is an SGSN) and/or saving (e.g., if the target PS node is an MME) additional information received from the second and/or third nodes (e.g., authentication vectors received from the second and/or third nodes). Saving the authentication vectors can be useful, for example, if the target PS node is an MME and a later handover will be made to the exact same source SGSN from which they were received (in which case, the authentication vectors are returned to the SGSN at the time of that later handover).

[0053] Additional aspects of embodiments consistent with the invention can be appreciated from FIG. 6, which is a signaling diagram of one embodiment consistent with the invention. In particular, this diagram focuses on aspects that support a target PS node being able to create a security context for a client as part of a handover of a call from source UTRAN or GERAN supporting equipment operating in the CS domain to target UTRAN supporting equipment operating in the PS domain. An aspect of the illustrated embodiment is that the target PS node collects security related information from the source PS node and also from the source CS node, and selected parts of the collected information are combined to generate a new set of security related information. This is described in greater detail in the following.

[0054] The illustrated components that participate in the signaling of this exemplary embodiment are a UE 601 (client), a source BSC/RNC 603, a target RNC 605, an MSC server 607, a source SGSN/MME 609, and a target SGSN 611.

[0055] Initially, the UE 601 is engaged in a CS call, supported by the various source UTRAN or GERAN equipment. In response to a decision being made to perform the CS (UTRAN or GERAN) to PS (UTRAN/GERAN) handover, in step 1" the source BSC/RNC 603 sends a "HO required" message to the MSC server 607.

[0056] The MSC server 607 then generates (step 613) a $NONCE_{MSC}$, and uses this and existing keys shared with the UE 601 to generate a cryptographic key in accordance with:

$$CK'_{PS} \,||\, IK'_{PS} = KDF(CK_{CS}, IK_{CS}, NONCE_{MSC}),$$

where the symbol "||" represents a concatenation function.

[0057] In step 2", the MSC server 607 communicates a "CS to PS HO request" to the target SGSN 611, and includes the generated cryptographic key ($CK'_{PS} \,||\, IK'_{PS}$) and authentication vectors in this message.

[0058] In response, in step 3" the target SGSN 611 sends a "Context request" to the source SGSN/MME 609 for the purpose of requesting context information for the UE 601. (Dashed lines used here and in other representations of signaling represent an optional step.) The SGSN/MME 609 then sends a "Context response" (including the requested information which includes the PS cryptographic keys and other security parameters such as the IDs of security algorithms

supported by the UE 601) back to the target SGSN 611 (step 4").

[0059] In step 615, the target SGSN 611 performs:

- Sending the cryptographic keys received from the MSC 607 to the target RNC 605 for the purpose of protecting traffic between the target SGSN 611 and the UE 601 (i.e., the client)
- Discarding any PS keys received from the source SGSN/MME 609
- Discarding the AVs that were received from the MSC server 607
- In some but not necessarily all embodiments, storing AVs received from the source SGSN 609
- In some but not necessarily all. embodiments, the data in the AVs may be used to re-authenticate the UE 601
- Using other information received from the source SGSN/MME 609 needed to create a new security context for the client (i.e., the UE 601)

[0060] Following step 615, the signaling is in accordance with steps 5, 6, 7, 8, 9, and 10 such as are shown in FIG. 3 and described in FIG. 3's supporting text above.

[0061] Other aspects of embodiments consistent with the invention can be appreciated from FIG. 7, which is a signaling diagram of an alternative embodiment consistent with the invention. In particular, this diagram focuses on aspects that support a target PS node being able to create a security context for a client as part of a handover of a call from source UTRAN or GERAN supporting equipment operating in the CS domain to target E-UTRAN (i.e., 4G) supporting equipment operating in the PS domain. The illustrated components that participate in this signaling are a UE 701 (client), a source BSC/RNC 703, a target eNB 705, an MSC server 707, a source SGSN/MME 709, and a target MME 711.

[0062] Initially, the UE 701 is engaged in a CS call, supported by the various source UTRAN or GERAN equipment. In response to a decision being made to perform the CS (UTRAN or GERAN) to PS (E-UTRAN) handover, in step 1"' the source BSC/RNC 703 sends a "HO required" message to the MSC server 707.

[0063] The MSC server 707 then generates (step 713) a $NONCE_{MSC}$, and uses this to generate new cryptographic keys from existing keys shared with the UE 701. This key derivation is in accordance with:

$$CK'_{PS} \,||\, IK'_{PS} = KDF(CK_{CS}, IK_{CS}, NONCE_{MSC}),$$

where the symbol "||" represents a concatenation function.

[0064] In step 2"', the MSC server 707 communicates a "CS to PS HO request" to the target MME 711, and includes the newly generated cryptographic keys ($CK'_{PS} \,||\, IK'_{PS}$) and AVs in this message. It will be observed that the MSC server 707 does not have LTE security parameters, so none are (or can be) transferred in this communication.

[0065] In response, in step 3'" the target MME 711 sends a "Context request" to the source SGSN/MME 709 for the purpose of requesting context information for the UE 701. The SGSN/MME 709 then sends a "Context response" (including the requested information) back to the target MME 711 (step 4"'). This requested information includes PS keys and LTE security parameters (i.e., IDs of LTE security algorithms that are supported by the UE 701). In the context of a source SGSN 709, such information is available if the source SGSN 709 complies with Release 8 or newer of the LTE standard.

[0066] In step 715, the target MME 711 performs:

- Creating a mapped EPS security context by setting the K'_{ASME} of the mapped EPS security context equal to the concatenation $CK'_{PS} \,||\, IK'_{PS}$, where the CK'_{PS} and were received in the CS to PS handover request (see step 2"'). The target MME 711 further associates the K'_{ASME} with a KSI_{SGSN}. The value of the KSI_{SGSN} is the same as the value of the KSI'_{PS} received in the CS to PS handover request. Also as part of this step, the target MME 711 derives K_{eNB} by applying the KDF as defined in the applicable standard, using the mapped key K'_{ASME} and 2^{32}-1 as the value of the uplink NAS COUNT parameter. The uplink and downlink NAS COUNT values for the mapped EPS security context are set to start value (i.e., 0) in the target MME 711.
- Discarding PS keys received from the source SGSN/MME 709
- Discarding AVs received from the MSC server 707
- Optionally storing AVs received from a source SGSN 709. (There will not be any AVs received from a source MME 709.) These stored AVs can later be used if there is to be a PS IRAT HO back to the very same source SGSN 709 as the one from which they were received (in which case they are transferred back to that SGSN at the time of that later handover).
- Using other information received from the source SGSN/MME 709 needed to create an LTE security context for the UE 701 (i.e., for the client). Such additional information can be, for example, the KSI or the CKSN, each of which is a 3-bit long string. For example, the MME 711 can use the KSI/CKSN to identify the security context in LTE.

[0067] Following step 715, the signaling is in accordance with steps 5', 6', 7', 8', 9', and 10' such as are shown in FIG. 4 and described in FIG. 4's supporting text above.

[0068] FIG. 8 is a block diagram of a target node 800 (e.g., SGSN/MME) that operates in the PS domain, wherein the target node 800 comprises a controller 801 that is circuitry configured to carry out, in addition to typical communications system node functionality, any one or any combination of the aspects described in connection with any one or combination of FIGS. 5 through 7 above. Such circuitry could, for example, be entirely hard-wired circuitry (e.g., one or more ASICs). Depicted in the exemplary embodiment of FIG. 8, however, is programmable circuitry, comprising a processor 803 coupled to one or more memory devices 805 (e.g., Random Access Memory, Magnetic Disc Drives, Optical Disk Drives, Read Only Memory, etc.). The memory device(s) 805 store program means 807 (e.g., a set of processor instructions) configured to cause the processor 803 to control other node circuitry/hardware components 809 so as to carry out any of the functions described above. The memory 805 may also store data 811 representing various constant and variable parameters as may be received, generated, and/or otherwise needed by the processor 803 when carrying out its functions such as those specified by the program means 807.

[0069] The various aspects of embodiments consistent with the invention as described above provide solutions to the problems relating to the handover of calls between CS and PS equipment, including the problem of how to generate a security context that is useful in the PS domain when the call has originated in the CS domain.

[0070] The invention has been described with reference to particular embodiments. However, it will be readily apparent to those skilled in the art that it is possible to embody the invention in specific forms other than those of the embodiment described above.

[0071] For example, the various aspects, such as obtaining some information from a source CS node and other information from a source PS node and filtering and/or processing this information to derive a security context that is useful in the target PS node are applicable even when some other details have changed. As an example, embodiments can be foreseen in which, instead of having an MSC generate a NONCE that is communicated to the target PS node (e.g., target SGSN or MME), the target node (target MME) can generate a NONCE itself, and then derive cryptographic keys from this generated NONCE.

[0072] Accordingly, the described embodiments are merely illustrative and should not be considered restrictive in any way. The scope of the invention is given by the appended claims, rather than the preceding description, and all variations and equivalents which fall within the range of the claims are intended to be embraced therein.

Claims

1. A method of operating a target packet switched node (611, 711, 800) to generate a security context for a client (201, 601, 701) in a cellular communication system as part of a handover of a circuit switched connection from a source circuit switched node to the target packet switched node (611, 711, 800), wherein the target packet switched node (611, 711, 800) comprises processing circuitry (801), the method comprising:

the target packet switched node (611, 711, 800) performing:

receiving (501) at least one cryptographic key from the source circuit switched node (607, 707);
receiving (503) identities of security algorithms supported by the client (601, 701) from a source packet switched node (609, 709); and
using (505) the at least one cryptographic key and the identities to generate the security context for the client (601, 701).

2. The method of claim 1, wherein the target packet switched node (611, 711, 800) is an MME, the source circuit switched node (607, 707) is an MSC and the source packet switched node (609, 709) is an SGSN.

3. The method of claim 1, wherein the target packet switched node (611, 711, 800) is a first SGSN, the source circuit switched node (607, 707) is an MSC and the source packet switched node (609, 709) is a second SGSN.

4. The method of claim 1, further comprising:

causing the target packet switched node (611, 711, 800) to receive (2"') one or more authentication vectors from the source circuit switched node (607, 707) when receiving (501) the at least one cryptographic key; and discarding (507) the authentication vectors received from the source circuit switched node (607, 707) when having used (505) the at least one cryptographic key and the identities to generate the security context for the client (601, 701).

5. The method of claim 1, wherein the target packet switched node (611, 711, 800) is an SGSN, and wherein the method further comprises:

using (507, 615) one or more of the at least one cryptographic key to protect traffic between a fourth node and the client (601, 701).

6. The method of claim 1, wherein the target packet switched node (611, 711, 800) is an MME, and wherein the method further comprises:

deriving (507, 715) a key for an Access Security Management Entity (K_ASME) from one or more of the at least one cryptographic key.

7. The method of claim 1, further comprising:

receiving (4", 4"'), from the source packet switched node (609, 709) when receiving (503) identities of security algorithms supported by the client (601, 701), packet switched encryption keys for use in a packet switched connection; and
discarding (507, 615, 715) the packet switched encryption keys when having used (505) the at least one cryptographic key and the identities to generate the security context for the client (601, 701).

8. The method of claim 1, further comprising:

receiving (4", 4"') at least one authentication vector from the source packet switched node (609, 709); and
storing (507, 615, 715) the received at least one authentication vector.

9. The method of claim 1, further comprising receiving additional information from the source packet switched node (609, 709); and
wherein using (505) the at least one cryptographic key and the identities to generate the security context for the client (601, 701) comprises using (505) the at least one cryptographic key and the identities and the additional information to generate the security context for the client (601, 701).

10. A method of operating target packet switched and source circuit switched nodes (611, 711, 800, 607, 707) in a cellular communication system (101) as part of a handover of a circuit switched connection from a source circuit switched node (607, 707) to the target packet switched node (611, 711, 800), the method operating to generate a security context as part of a process of handing over support of a client (601, 701) from the source circuit switched node (607, 707) to the target packet switched node (611, 711, 800), wherein the target packet switched and source circuit switched nodes (611, 711, 800, 607, 707) each comprise processing circuitry, the method**characterized by**:

the source circuit switched node (607, 707) generating (613, 713) at least one new cryptographic key from at least one existing key associated with the client (601, 701) and a nonce generated by the source circuit switched node (607, 707);
the source circuit switched node (607, 707) communicating (2", 2"', 501) the at least one new cryptographic key to the target packet switched node (611, 711, 800);
the target packet switched node (611, 711, 800) receiving (503) identities of security algorithms supported by the client (601, 701) from a source packet switched node (609, 709); and
the target packet switched node (611, 711, 800) using (505) the at least one cryptographic key and the identities to generate the security context for the client (601, 701).

11. An apparatus (500, 801) for operating a target packet switched node (611, 711, 800) to generate a security context for a client (601, 701) in a cellular communication system (101) as part of a handover of a circuit switched connection from a source circuit switched node (607, 707) to the target packet switched node (611, 711, 800), the apparatus comprising:

circuitry (501) configured to receive at least one cryptographic key from the source circuit switched node (607, 707);
circuitry (503) configured to receive identities of security algorithms supported by the client (601, 701) from a source packet switched node (609, 709); and
circuitry (505) configured to use the at least one cryptographic key and the identities to generate the security

context for the client (601, 701).

12. The apparatus of claim 11, wherein the target packet switched node (611, 711, 800) is an MME, the source circuit switched node (607, 707) is an MSC and the source packet switched node (609, 709) is an SGSN.

13. The apparatus of claim 11, wherein the target packet switched node (611, 711, 800) is a first SGSN, the source circuit switched node (607, 707) is an MSC and the source packet switched node (609, 709) is a second SGSN.

14. The apparatus of claim 11, further comprising:

circuitry configured to receive (2"') one or more authentication vectors from the source circuit switched node (607, 707) when receiving (501) the at least one cryptographic key; and
circuitry configured to discard (507) the authentication vectors received from the source circuit switched node (607, 707) when having used (505) the at least one cryptographic key and the identities to generate the security context for the client (601, 701).

15. The apparatus of claim 11, wherein the target packet switched node (611, 711, 800) is an SGSN, and wherein the apparatus further comprises:

circuitry configured to use (507, 615) one or more of the at least one cryptographic key to protect traffic between a fourth node and the client (601, 701).

16. The apparatus of claim 11, wherein the target packet switched node (611, 711, 800) is an MME, and wherein the apparatus further comprises:

circuitry configured to derive (507, 715) a key for an Access Security Management Entity (K_ASME) from one or more of the at least one cryptographic key.

17. The apparatus of claim 11, further comprising:

circuitry configured to receive (4", 4"'), from the source packet switched node (609, 709) when receiving (503) identities of security algorithms supported by the client (601, 701), packet switched encryption keys for use in a packet switched connection; and
circuitry configured to discard (507, 615, 715) the packet switched encryption keys when having used (505) the at least one cryptographic key and the identities to generate the security context for the client (601, 701).

18. The apparatus of claim 11, further comprising:

circuitry configured to receive (4", 4"') at least one authentication vector from the source packet switched node (609, 709); and
circuitry configured to store (507, 615, 715) the received at least one authentication vector.

19. The apparatus of claim 11, further comprising circuitry configured to receive additional information from the source packet switched node (609, 709); and
wherein the circuitry configured to use (505) the at least one cryptographic key and the identities to generate the security context for the client (601, 701) comprises circuitry configured to use (505) the at least one cryptographic key and the identities and the additional information to generate the security context for the client (601, 701).

20. A system for operating target packet switched and source circuit switched nodes (611, 711, 800, 607, 707) in a cellular communication system (101) as part of a handover of a circuit switched connection from a source circuit switched node (607, 707) to the target packet switched node (611, 711, 800), the system operating to generate a security context as part of a process of handing over support of a client (601, 701) from the source circuit switched node (607, 707) to the target packet switched node (611, 711, 800), the system comprising :

source circuit switched node circuitry configured to generate (613, 713) at least one new cryptographic key from at least one existing key associated with the client (601, 701) and a nonce generated by the source circuit switched node (607, 707);
source circuit switched node circuitry configured to communicate (2", 2"', 501) the at least one new cryptographic

key to the target packet switched node (611, 711, 800);
target packet switched node (611, 711, 800) circuitry configured to receive (503) identities of security algorithms supported by the client (601, 701) from a source packet switched node (609, 709);
target packet switched node (611, 711, 800) circuitry configured to use (505) the at least one cryptographic key and the identities to generate the security context for the client (601, 701).

Patentansprüche

1. Verfahren zum Betreiben eines paketvermittelten Zielkknotens (611, 711, 800) zum Erzeugen eines Sicherheitskontexts für einen Client (201, 601, 701) in einem zellularen Kommunikationssystem als Teil einer Übergabe einer kreisvermittelten Verbindung von einem kreisvermittelten Quellknoten zu dem paketvermittelten Knoten (611, 711, 800), wobei der paketvermittelte Zielknoten (611, 711, 800) Verarbeitungsschaltlogik (801) umfasst, wobei das Verfahren Folgendes umfasst:

   Ausführen durch den paketvermittelten Zielkknoten (611, 711, 800) von Folgendem:

   Empfangen (501) wenigstens eines kryptographischen Schlüssels von dem kreisvermitteltem Quellknoten (607, 707);
   Empfangen (503) von Identitäten von Sicherheitsalgorithmen, die von dem Client (601, 701) unterstützt werden, von einem paketvermittelten Quellknoten (609, 709); und
   Verwenden (505) des mindestens einen kryptographischen Schlüssels und der Identitäten, um den Sicherheitskontext für den Client (601, 701) zu erzeugen.

2. Verfahren nach Anspruch 1, wobei der paketvermittelte Zielkknoten (611,711, 800) ein MME ist, der kreisvermittelte Quellknoten (607, 707) ein MSC ist und der paketvermittelte Quellknoten (609, 709) ein SGSN ist.

3. Verfahren nach Anspruch 1, wobei der paketvermittelte Zielkknoten (611,711, 800) ein erster SGSN ist, der kreisvermittelte Quellknoten (607, 707) ein MSC ist und der paketvermittelte Quellknoten (609, 709) ein zweiter SGSN ist.

4. Verfahren nach Anspruch 1, ferner umfassend:

   Bewirken, dass der paketvermittelte Zielkknoten (611, 711, 800) einen oder mehrere Authentifizierungsvektoren von dem kreisvermittelten Quellknoten (607, 707) empfängt (2"'), wenn der mindestens eine kryptographische Schlüssel empfangen (501) wird; und
   Verwerfen (507) der von dem kreisvermittelten Quellknoten (607, 707) empfangenen Authentifizierungsvektoren, wenn der mindestens eine kryptographische Schlüssel und die Identitäten verwendet wurden (505), um den Sicherheitskontext für den Client (601, 701) zu erzeugen.

5. Verfahren nach Anspruch 1, wobei der paketvermittelte Zielkknoten (611,711, 800) ein SGSN ist und wobei das Verfahren ferner Folgendes umfasst:

   Verwenden (507, 615) eines oder mehrerer des mindestens einen kryptographischen Schlüssels, um Verkehr zwischen einem vierten Knoten und dem Client (601, 701) zu schützen.

6. Verfahren nach Anspruch 1, wobei der paketvermittelte Zielkknoten (611,711, 800) ein MME ist und wobei das Verfahren ferner Folgendes umfasst:

   Ableiten (507, 715) eines Schlüssels für eine Zugriffssicherheitsverwaltungsentität (Access Security Management Entity) (K_ASME) aus einem oder mehreren des mindestens einen kryptographischen Schlüssels.

7. Verfahren nach Anspruch 1, ferner umfassend:

   wenn Identitäten von Sicherheitsalgorithmen, die durch den Client (601, 701) unterstützt werden, empfangen werden (503), Empfangen (4", 4"') von dem paketvermittelten Quellknoten (609, 709) von paketvermittelten Verschlüsselungsschlüsseln zur Verwendung in einer paketvermittelten Verbindung; und
   Verwerfen (507, 615, 715) der paketvermittelten Verschlüsselungsschlüssel, wenn der mindestens eine kryptographische Schlüssel und die Identitäten verwendet wurden (505), um den Sicherheitskontext für den Client

(601, 701) zu erzeugen.

8. Verfahren nach Anspruch 1, ferner umfassend:

Empfangen (4", 4"') mindestens eines Authentifizierungsvektors von dem paketvermittelten Quellknoten (609, 709); und
Speichern (507, 615, 715) des empfangenen mindestens einen Authentifizierungsvektors.

9. Verfahren nach Anspruch 1, ferner umfassend Empfangen zusätzlicher Informationen von dem paketvermittelten Quellknoten (609, 709); und
wobei das Verwenden (505) des mindestens einen kryptographischen Schlüssels und der Identitäten, um den Sicherheitskontext für den Client (601, 701) zu erzeugen, das Verwenden (505) des mindestens einen kryptographischen Schlüssels und der Identitäten und der zusätzlichen Informationen umfasst, um den Sicherheitskontext für den Client (601, 701) zu erzeugen.

10. Verfahren zum Betreiben von paketvermittelten Zielknoten und kreisvermittelten Quellknoten (611,711, 800, 607, 707) in einem zellularen Kommunikationssystem (101) als Teil einer Übergabe einer kreisvermittelten Verbindung von einem kreisvermittelten Quellknoten (607, 707) an den paketvermittelten Zielknoten (611, 711, 800), wobei das Verfahren arbeitet, um einen Sicherheitskontext als Teil eines Prozesses zum Übergeben der Unterstützung eines Clients (601, 701) von dem kreisvermittelten Quellknoten (607, 707) an den paketvermittelten Zielknoten (611,711, 800) zu erzeugen, wobei die paketvermittelten Zielknoten (611, 711, 800, 607, 707) der Zielschaltung jeweils eine Verarbeitungsschaltlogik umfassen, wobei das Verfahren **gekennzeichnet ist durch**:

durch den kreisvermittelten Quellknoten (607, 707), Erzeugen (613, 713) mindestens eines neuen kryptographischen Schlüssels aus mindestens einem mit dem Client (601, 701) assoziierten bestehenden Schlüssel und einer von dem kreisvermittelten Quellknoten (607, 707) erzeugten Nonce;
durch den kreisvermittelten Quellknoten (607, 707), Kommunizieren (2", 2"', 501) des mindestens einen neuen kryptographischen Schlüssels an den paketvermittelten Zielkknoten (611,711, 800);
durch den paketvermittelten Zielkknoten (611,711, 800), Empfangen (503) von Identitäten von Sicherheitsalgorithmen, die von dem Client (601, 701) unterstützt werden, von einem paketvermittelten Quellknoten (609, 709); und
durch den paketvermittelten Zielkknoten (611,711, 800), Verwenden (505) des mindestens einen kryptographischen Schlüssels und der Identitäten, um den Sicherheitskontext für den Client (601, 701) zu erzeugen.

11. Einrichtung (500, 801) zum Betreiben eines paketvermittelten Zielkknotens (611,711, 800) zum Erzeugen eines Sicherheitskontexts für einen Client (601, 701) in einem zellularen Kommunikationssystem (101) als Teil einer Übergabe einer kreisvermittelten Verbindung von einem kreisvermittelten Knoten (607, 707) zu dem paketvermittelten Knoten (611, 711, 800), wobei die Einrichtung Folgendes umfasst:

Schaltlogik (501), die konfiguriert ist zum Empfangen wenigstens eines kryptographischen Schlüssels von dem kreisvermittelten Quellknoten (607, 707);
Schaltlogik (503), die konfiguriert ist zum Empfangen von Identitäten von Sicherheitsalgorithmen, die von dem Client (601, 701) unterstützt werden, von einem paketvermittelten Quellknoten (609, 709); und
Schaltlogik (505), die konfiguriert ist zum Verwenden des mindestens einen kryptographischen Schlüssels und der Identitäten, um den Sicherheitskontext für den Client (601, 701) zu erzeugen.

12. Einrichtung nach Anspruch 11, wobei der paketvermittelte Zielkknoten (611,711, 800) ein MME ist, der kreisvermittelte Quellknoten (607, 707) ein MSC ist und der paketvermittelte Quellknoten (609, 709) ein SGSN ist.

13. Einrichtung nach Anspruch 11, wobei der paketvermittelte Zielkknoten (611,711, 800) ein erster SGSN ist, der kreisvermittelte Quellknoten (607, 707) ein MSC ist und der paketvermittelte Quellknoten (609, 709) ein zweiter SGSN ist.

14. Einrichtung nach Anspruch 11, ferner umfassend:

Schaltlogik, die konfiguriert ist zum Empfangen (2"') eines oder mehrerer Authentifizierungsvektoren von dem kreisvermittelten Quellknoten (607, 707), wenn der mindestens eine kryptographische Schlüssel empfangen (501) wird; und

Schaltlogik, die konfiguriert ist zum Verwerfen (507) der von dem kreisvermittelten Quellknoten (607, 707) empfangenen Authentifizierungsvektoren, wenn der mindestens eine kryptographische Schlüssel und die Identitäten verwendet wurden (505), um den Sicherheitskontext für den Client (601, 701) zu erzeugen.

15. Einrichtung nach Anspruch 11, wobei der paketvermittelte Zielkknoten (611,711, 800) ein SGSN ist und wobei die Einrichtung ferner Folgendes umfasst:

Schaltlogik, die konfiguriert ist zum Verwenden (507, 615) eines oder mehrerer des mindestens einen kryptographischen Schlüssels, um Verkehr zwischen einem vierten Knoten und dem Client (601, 701) zu schützen.

16. Einrichtung nach Anspruch 11, wobei der paketvermittelte Zielkknoten (611, 711, 800) eine MME ist und wobei die Einrichtung ferner Folgendes umfasst:

Schaltlogik, die konfiguriert ist zum Ableiten (507, 715) eines Schlüssels für eine Zugriffssicherheitsverwaltungsentität (Access Security Management Entity) (K_ASME) aus einem oder mehreren des mindestens einen kryptographischen Schlüssels.

17. Einrichtung nach Anspruch 11, ferner umfassend:

Schaltlogik, die konfiguriert ist, zum Empfangen (4", 4"') von dem paketvermittelten Quellknoten (609, 709) von paketvermittelten Verschlüsselungsschlüsseln zur Verwendung in einer paketvermittelten Verbindung, wenn Identitäten von Sicherheitsalgorithmen, die durch den Client (601, 701) unterstützt werden, empfangen werden (503); und
Schaltlogik, die konfiguriert ist, zum Verwerfen (507, 615, 715) der paketvermittelten Verschlüsselungsschlüssel, wenn der mindestens eine kryptographische Schlüssel und die Identitäten verwendet wurden (505), um den Sicherheitskontext für den Client (601, 701) zu erzeugen.

18. Einrichtung nach Anspruch 11, ferner umfassend:

Schaltlogik, die konfiguriert ist, zum Empfangen (4", 4"') mindestens eines Authentifizierungsvektors von dem paketvermittelten Quellknoten (609, 709); und
Schaltlogik, die konfiguriert ist, zum Speichern (507, 615, 715) des empfangenen mindestens einen Authentifizierungsvektors.

19. Einrichtung nach Anspruch 11, ferner umfassend Schaltlogik, die konfiguriert ist, zum Empfangen zusätzlicher Informationen von dem paketvermittelten Quellknoten (609, 709); und
wobei die Schaltlogik, die konfiguriert ist zum Verwenden (505) des mindestens einen kryptographischen Schlüssels und der Identitäten, um den Sicherheitskontext für den Client (601, 701) zu erzeugen, Schaltlogik umfasst, die konfiguriert ist zum Verwenden (505) des mindestens einen kryptographischen Schlüssels und der Identitäten und der zusätzlichen Informationen, um den Sicherheitskontext für den Client (601, 701) zu erzeugen.

20. System zum Betreiben von paketvermittelten Zielknoten und kreisvermittelten Quellknoten (611, 711, 800, 607, 707) in einem zellularen Kommunikationssystem (101) als Teil einer Übergabe einer kreisvermittelten Verbindung von einem kreisvermittelten Quellknoten (607, 707) an den paketvermittelten Zielknoten (611,711, 800), wobei das System arbeitet, um einen Sicherheitskontext als Teil eines Prozesses zum Übergeben der Unterstützung eines Clients (601, 701) von dem kreisvermittelten Quellknoten (607, 707) an den paketvermittelten Zielknoten (611,711, 800) zu erzeugen, wobei das System Folgendes umfasst:

kreisvermittelte Quellknotenschaltlogik, die konfiguriert ist zum Erzeugen (613, 713) mindestens eines neuen kryptographischen Schlüssel aus mindestens einem mit dem Client (601, 701) assoziierten bestehenden Schlüssel und einer von dem kreisvermittelten Quellknoten (607, 707) erzeugten Nonce;
kreisvermittelte Quellknotenschaltlogik, die konfiguriert ist zum Kommunizieren (2", 2"', 501) des mindestens einen neuen kryptographischen Schlüssels an den paketvermittelten Zielkknoten (611,711, 800);
paketvermittelte Zielkknoten- (611,711, 800) Schaltlogik, die konfiguriert ist zum Empfangen (503) von Identitäten von Sicherheitsalgorithmen, die von dem Client (601, 701) unterstützt werden, von einem paketvermittelten Quellknoten (609, 709);
paketvermittelte Zielkknoten- (611,711, 800) Schaltlogik, die konfiguriert ist zum Verwenden (505) des mindestens einen kryptographischen Schlüssels und der Identitäten, um den Sicherheitskontext für den Client (601,

701) zu erzeugen.

Revendications

1. Procédé d'exploitation d'un noeud à commutation de paquets cible (611, 711, 800) pour générer un contexte de sécurité pour un dispositif client (201, 601, 701) dans un système de communication cellulaire dans le cadre d'un transfert intercellulaire d'une connexion à commutation de circuits d'un noeud à commutation de circuits source à un noeud à commutation de paquets cible (611, 711, 800), dans lequel le noeud à commutation de paquets cible (611, 711, 800) comprend un montage de circuits de traitement (801), le procédé comprenant les étapes ci-dessous consistant à, mises en oeuvre par le noeud à commutation de paquets cible (611, 711, 800) :

   recevoir (501) au moins une clé cryptographique en provenance du noeud à commutation de circuits source (607, 707) ;
   recevoir (503) des identités d'algorithmes de sécurité pris en charge par le dispositif client (601, 701) en provenance d'un noeud à commutation de paquets source (609, 709) ; et
   utiliser (505) ladite au moins une clé cryptographique et les identités en vue de générer le contexte de sécurité pour le dispositif client (601, 701).

2. Procédé selon la revendication 1, dans lequel le noeud à commutation de paquets cible (611, 711, 800) est une entité de gestion de la mobilité, MME, le noeud à commutation de circuits source (607, 707) est un centre de commutation du service des mobiles, MSC, et le noeud à commutation de paquets source (609, 709) est un noeud de support GPRS de service, SGSN.

3. Procédé selon la revendication 1, dans lequel le noeud à commutation de paquets cible (611, 711, 800) est un premier noeud SGSN, le noeud à commutation de circuits source (607, 707) est un centre MSC et le noeud à commutation de paquets source (609, 709) est un second noeud SGSN.

4. Procédé selon la revendication 1, comprenant en outre les étapes ci-dessous consistant à :

   amener le noeud à commutation de paquets cible (611, 711, 800) à recevoir (2"') un ou plusieurs vecteurs d'authentification en provenance du noeud à commutation de circuits source (607, 707) dans le cadre de la réception (501) de ladite au moins une clé cryptographique ; et
   rejeter (507) les vecteurs d'authentification reçus en provenance du noeud à commutation de circuits source (607, 707) après avoir utilisé (505) ladite au moins une clé cryptographique et les identités en vue de générer le contexte de sécurité pour le dispositif client (601, 701).

5. Procédé selon la revendication 1, dans lequel le noeud à commutation de paquets cible (611, 711, 800) est un noeud SGSN, et dans lequel le procédé comprend en outre l'étape ci-dessous consistant à :

   utiliser (507, 615) une ou plusieurs clés de ladite au moins une clé cryptographique pour protéger le trafic entre un quatrième noeud et le dispositif client (601, 701).

6. Procédé selon la revendication 1, dans lequel le noeud à commutation de paquets cible (611, 711, 800) est une entité MME, et dans lequel le procédé comprend en outre l'étape ci-dessous consistant à :

   dériver (507, 715) une clé pour une entité de gestion de sécurité d'accès (K ASME) à partir d'une ou de plusieurs clés de ladite au moins une clé cryptographique.

7. Procédé selon la revendication 1, comprenant en outre les étapes ci-dessous consistant à :

   recevoir (4", 4"'), en provenance du noeud à commutation de paquets source (609, 709), dans le cadre de la réception (503) d'identités d'algorithmes de sécurité pris en charge par le dispositif client (601, 701), des clés de chiffrement à commutation de paquets destinées à être utilisées dans une connexion à commutation de paquets ; et
   rejeter (507, 615, 715) les clés de chiffrement à commutation de paquets après avoir utilisé (505) ladite au moins une clé cryptographique et les identités en vue de générer le contexte de sécurité pour le dispositif client (601, 701).

8. Procédé selon la revendication 1, comprenant en outre les étapes ci-dessous consistant à :

recevoir (4", 4"') au moins un vecteur d'authentification en provenance du noeud à commutation de paquets source (609, 709) ; et
stocker (507, 615, 715) ledit au moins un vecteur d'authentification reçu.

9. Procédé selon la revendication 1, comprenant en outre l'étape consistant à recevoir des informations supplémentaires en provenance du noeud à commutation de paquets source (609, 709) ; et
dans lequel l'étape d'utilisation (505) de ladite au moins une clé cryptographique et des identités en vue de générer le contexte de sécurité pour le dispositif client (601, 701) consiste à utiliser (505) ladite au moins une clé cryptographique, les identités, et les informations supplémentaires en vue de générer le contexte de sécurité pour le dispositif client (601, 701).

10. Procédé d'exploitation de noeuds à commutation de circuits source et à commutation de paquets cible (611, 711, 800, 607, 707) dans un système de communication cellulaire (101) dans le cadre d'un transfert intercellulaire d'une connexion à commutation de circuits d'un noeud à commutation de circuits source (607, 707) au noeud à commutation de paquets cible (611, 711, 800), le procédé étant exploitable de manière à générer un contexte de sécurité dans le cadre d'un processus de transfert de prise en charge d'un dispositif client (601, 701) du noeud à commutation de circuits source (607, 707) au noeud à commutation de paquets cible (611, 711, 800), dans lequel les noeuds à commutation de paquets cible et à commutation de circuits source (611, 711, 800, 607, 707) comprennent chacun un montage de circuits de traitement, le procédé étant **caractérisé en ce que** :

le noeud à commutation de circuits source (607, 707) génère (613, 713) au moins une nouvelle clé cryptographique à partir d'au moins une clé existante associée au dispositif client (601, 701) et un nonce généré par le noeud à commutation de circuits source (607, 707) ;
le noeud à commutation de circuits source (607, 707) communique (2", 2"', 501) ladite au moins une nouvelle clé cryptographique au noeud à commutation de paquets cible (611, 711, 800) ;
le noeud à commutation de paquets cible (611, 711, 800) reçoit (503) des identités d'algorithmes de sécurité pris en charge par le dispositif client (601, 701) en provenance d'un noeud à commutation de paquets source (609, 709) ; et
le noeud à commutation de paquets cible (611, 711, 800) utilise (505) ladite au moins une clé cryptographique et les identités en vue de générer le contexte de sécurité pour le dispositif client (601, 701).

11. Appareil (500, 801) destiné à exploiter un noeud à commutation de paquets cible (611, 711, 800) en vue de générer un contexte de sécurité pour un dispositif client (601, 701) dans un système de communication cellulaire (101) dans le cadre d'un transfert intercellulaire d'une connexion à commutation de circuits d'un noeud à commutation de circuits source (607, 707) au noeud à commutation de paquets cible (611, 711, 800), l'appareil comprenant :

un montage de circuits (501) configuré de manière à recevoir au moins une clé cryptographique en provenance du noeud à commutation de circuits source (607, 707) ;
un montage de circuits (503) configuré de manière à recevoir des identités d'algorithmes de sécurité pris en charge par le dispositif client (601, 701) en provenance d'un noeud à commutation de paquets source (609, 709) ; et
un montage de circuits (505) configuré de manière à utiliser au moins une clé cryptographique et les identités en vue de générer le contexte de sécurité pour le dispositif client (601, 701).

12. Appareil selon la revendication 11, dans lequel le noeud à commutation de paquets cible (611, 711, 800) est une entité de gestion de la mobilité, MME, le noeud à commutation de circuits source (607, 707) est un centre de commutation du service des mobiles, MSC, et le noeud à commutation de paquets source (609, 709) est un noeud de support GPRS de service, SGSN.

13. Appareil selon la revendication 11, dans lequel le noeud à commutation de paquets cible (611, 711, 800) est un premier noeud SGSN, le noeud à commutation de circuits source (607, 707) est un centre MSC et le noeud à commutation de paquets source (609, 709) est un second noeud SGSN.

14. Appareil selon la revendication 11, comprenant en outre :

un montage de circuits configuré de manière à recevoir (2"') un ou plusieurs vecteurs d'authentification en

provenance du noeud à commutation de circuits source (607, 707) dans le cadre de la réception (501) de ladite au moins une clé cryptographique ; et
un montage de circuits configuré de manière à rejeter (507) les vecteurs d'authentification reçus en provenance du noeud à commutation de circuits source (607, 707) après avoir utilisé (505) ladite au moins une clé cryptographique et les identités en vue de générer le contexte de sécurité pour le dispositif client (601, 701).

15. Appareil selon la revendication 11, dans lequel le noeud à commutation de paquets cible (611, 711, 800) est un noeud SGSN, et dans lequel l'appareil comprend en outre :

un montage de circuits configuré de manière à utiliser (507, 615) une ou plusieurs clés de ladite au moins une clé cryptographique en vue de protéger le trafic entre un quatrième noeud et le dispositif client (601, 701).

16. Appareil selon la revendication 11, dans lequel le noeud à commutation de paquets cible (611, 711, 800) est une entité MME, et dans lequel l'appareil comprend en outre :

un montage de circuits configuré de manière à dériver (507, 715) une clé pour une entité de gestion de sécurité d'accès (K ASME) à partir d'une ou plusieurs clés de ladite au moins une clé cryptographique.

17. Appareil selon la revendication 11, comprenant en outre :

un montage de circuits configuré de manière à recevoir (4", 4"'), en provenance du noeud à commutation de paquets source (609, 709), dans le cadre de la réception (503) d'identités d'algorithmes de sécurité pris en charge par le dispositif client (601, 701), des clés de chiffrement à commutation de paquets destinées à être utilisées dans une connexion à commutation de paquets ; et
un montage de circuits configuré de manière à rejeter (507, 615, 715) les clés de chiffrement à commutation de paquets après avoir utilisé (505) ladite au moins une clé cryptographique et les identités en vue de générer le contexte de sécurité pour le dispositif client (601, 701).

18. Appareil selon la revendication 11, comprenant en outre :

un montage de circuits configuré de manière à recevoir (4", 4"') au moins un vecteur d'authentification en provenance du noeud à commutation de paquets source (609, 709) ; et
un montage de circuits configuré de manière à stocker (507, 615, 715) ledit au moins un vecteur d'authentification reçu.

19. Appareil selon la revendication 11, comprenant en outre un montage de circuits configuré de manière à recevoir des informations supplémentaires en provenance du noeud à commutation de paquets source (609, 709) ; et
dans lequel le montage de circuits configuré de manière à utiliser (505) ladite au moins une clé cryptographique et les identités en vue de générer le contexte de sécurité pour le dispositif client (601, 701) comprend un montage de circuits configuré de manière à utiliser (505) ladite au moins une clé cryptographique, les identités, et les informations supplémentaires en vue de générer le contexte de sécurité pour le dispositif client (601, 701).

20. Système destiné à exploiter des noeuds à commutation de circuits source et à commutation de paquets cible (611, 711, 800, 607, 707) dans un système de communication cellulaire (101) dans le cadre d'un transfert intercellulaire d'une connexion à commutation de circuits d'un noeud à commutation de circuits source (607, 707) au noeud à commutation de paquets cible (611, 711, 800), le système étant exploitable de manière à générer un contexte de sécurité dans le cadre d'un processus de transfert de prise en charge d'un dispositif client (601, 701) du noeud à commutation de circuits source (607, 707) au noeud à commutation de paquets cible (611, 711, 800), le système comprenant :

un montage de circuits de noeud à commutation de circuits source configuré de manière à générer (613, 713) au moins une nouvelle clé cryptographique à partir d'au moins une clé existante associée au dispositif client (601, 701) et un nonce généré par le noeud à commutation de circuits source (607, 707) ;
un montage de circuits de noeud à commutation de circuits source configuré de manière à communiquer (2", 2'", 501) ladite au moins une nouvelle clé cryptographique au noeud à commutation de paquets cible (611, 711, 800) ;
un montage de circuits de noeud à commutation de paquets cible (611, 711, 800) configuré de manière à recevoir (503) des identités d'algorithmes de sécurité pris en charge par le dispositif client (601, 701) en pro-

venance d'un noeud à commutation de paquets source (609, 709) ; et
un montage de circuits de noeud à commutation de paquets cible (611, 711, 800) configuré de manière à utiliser (505) ladite au moins une clé cryptographique et les identités en vue de générer le contexte de sécurité pour le dispositif client (601, 701).

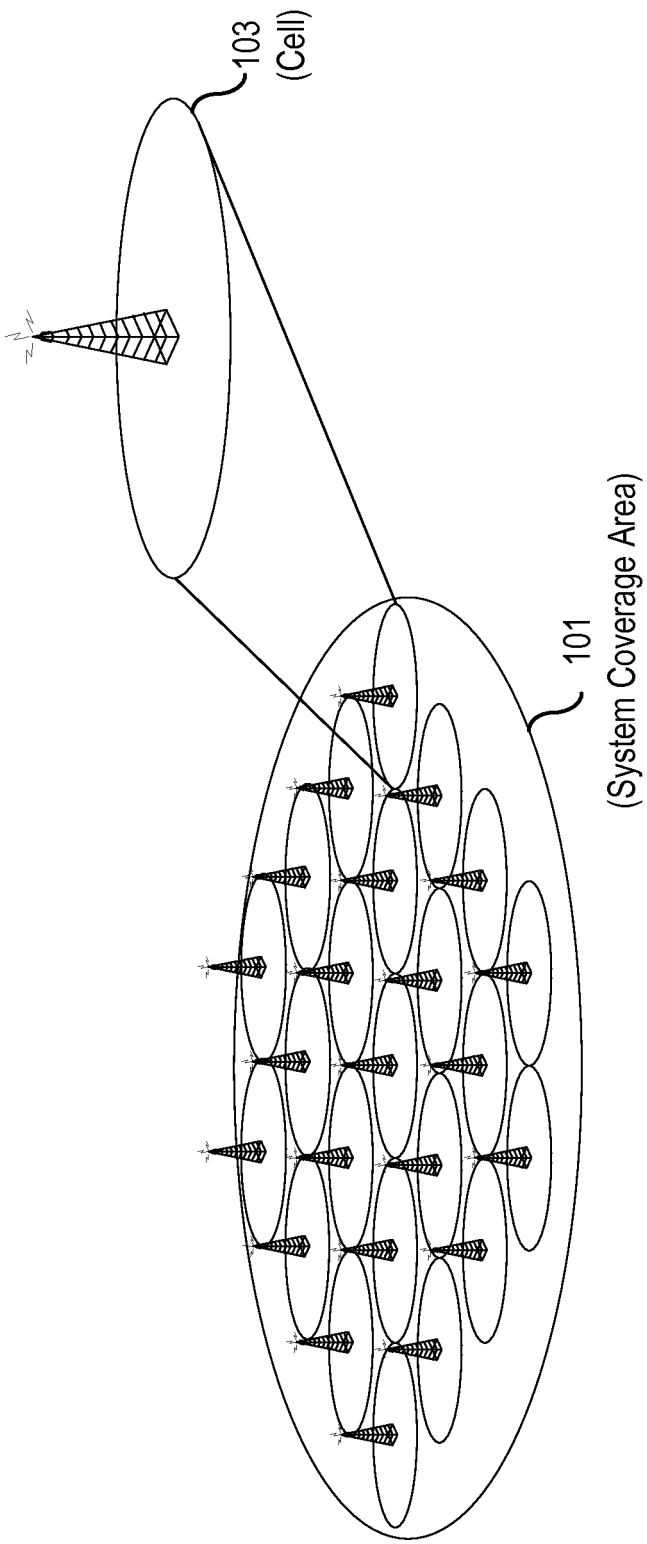

FIG. 1
(PriorArt)

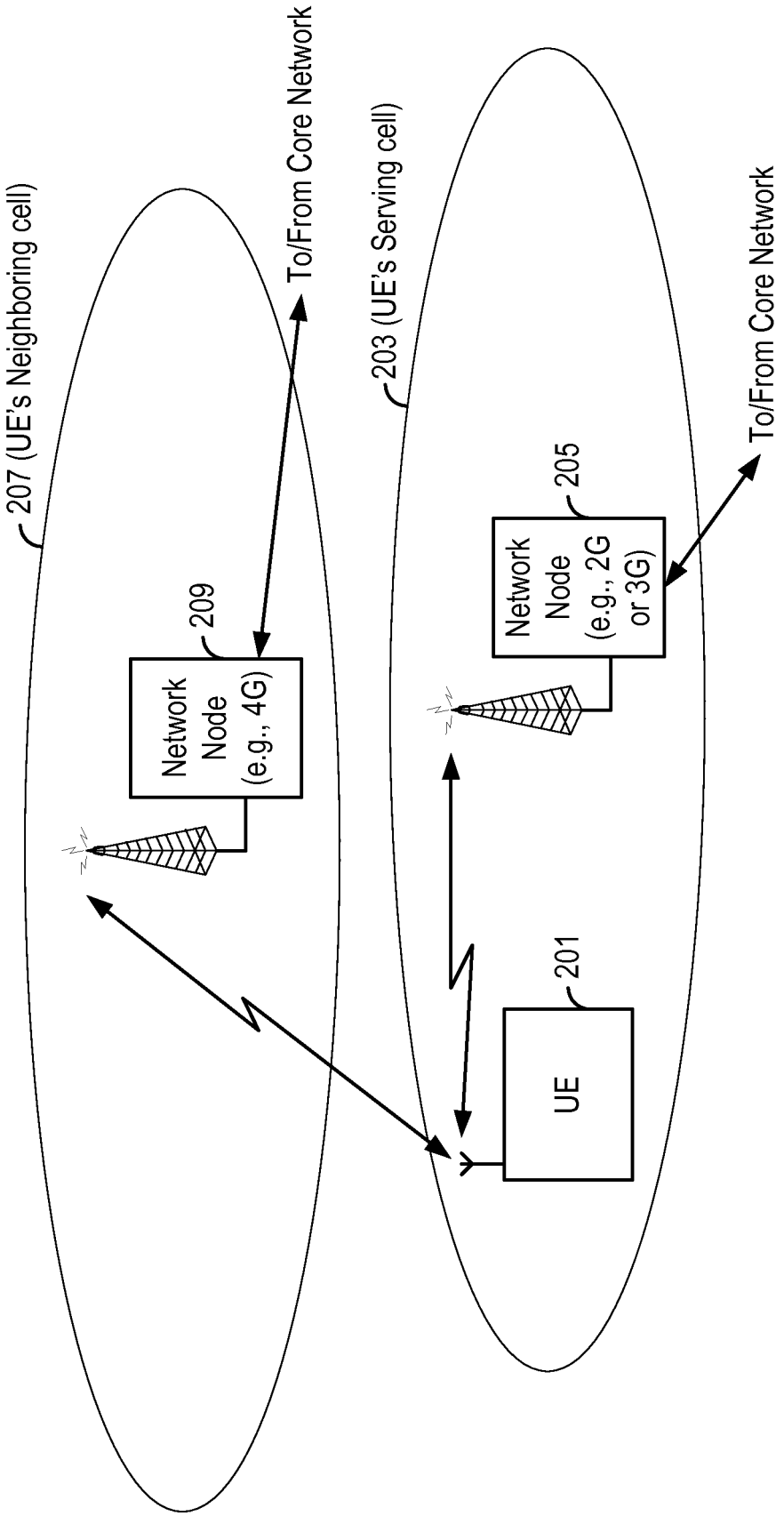
207 (UE's Neighboring cell)
To/From Core Network
209
Network Node (e.g., 4G)
203 (UE's Serving cell)
205
Network Node (e.g., 2G or 3G)
To/From Core Network
201
UE

FIG. 2

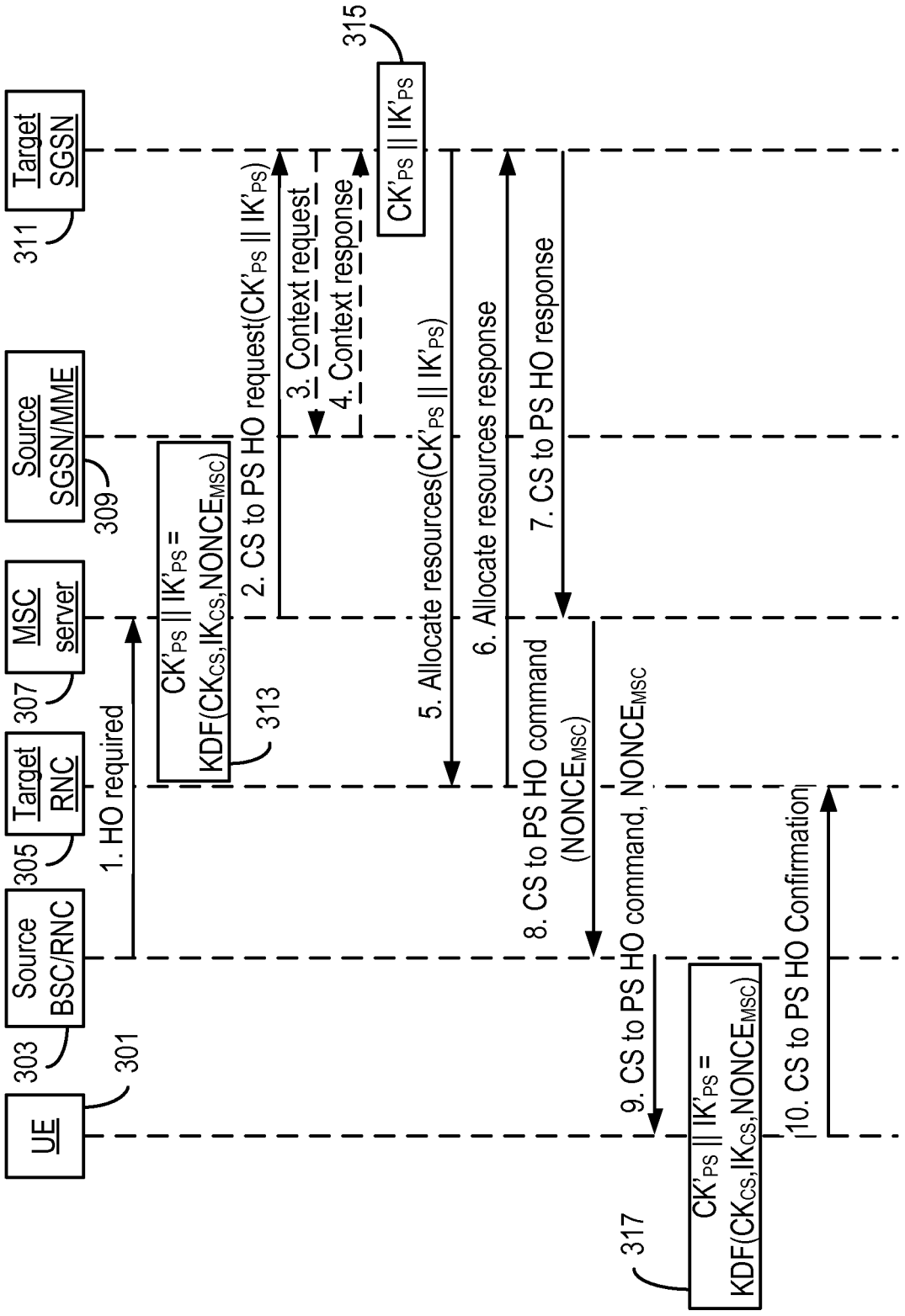
UE
301
Source BSC/RNC
303
Target RNC
305
MSC server
307
Source SGSN/MME
309
Target SGSN
311
1. HO required
2. CS to PS HO request(CK'PS || IK'PS)
3. Context request
4. Context response
315
CK'PS || IK'PS
313
CK'PS || IK'PS = KDF(CKCS,IKCS,NONCEMSC)
5. Allocate resources(CK'PS || IK'PS)
6. Allocate resources response
7. CS to PS HO response
8. CS to PS HO command (NONCEMSC)
9. CS to PS HO command, NONCEMSC
317
CK'PS || IK'PS = KDF(CKCS,IKCS,NONCEMSC)
10. CS to PS HO Confirmation

FIG. 3

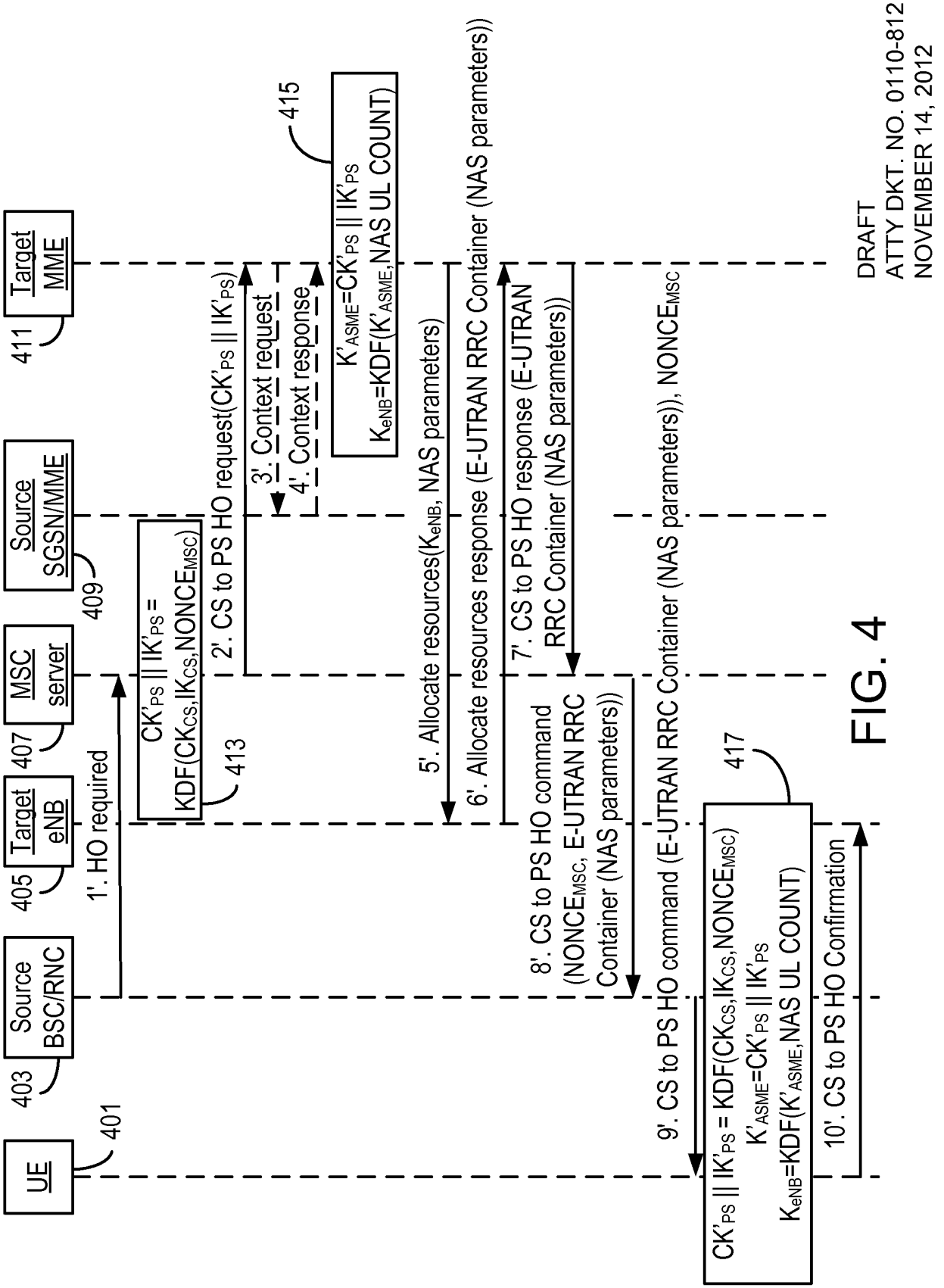

FIG. 4

DRAFT
ATTY DKT. NO. 0110-812
NOVEMBER 14, 2012

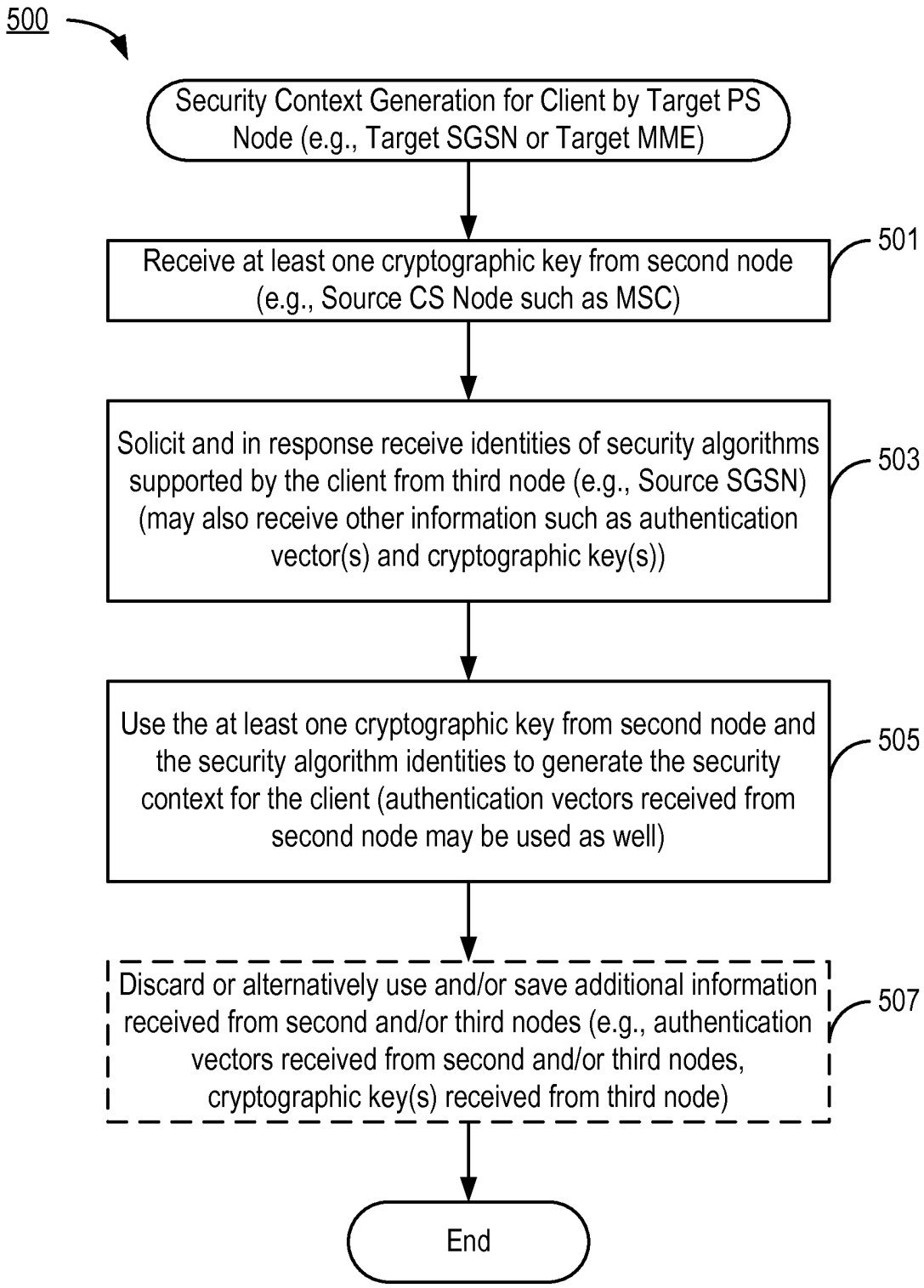
500
Security Context Generation for Client by Target PS Node (e.g., Target SGSN or Target MME)
Receive at least one cryptographic key from second node (e.g., Source CS Node such as MSC)
501
Solicit and in response receive identities of security algorithms supported by the client from third node (e.g., Source SGSN) (may also receive other information such as authentication vector(s) and cryptographic key(s))
503
Use the at least one cryptographic key from second node and the security algorithm identities to generate the security context for the client (authentication vectors received from second node may be used as well)
505
Discard or alternatively use and/or save additional information received from second and/or third nodes (e.g., authentication vectors received from second and/or third nodes, cryptographic key(s) received from third node)
507
End

FIG. 5

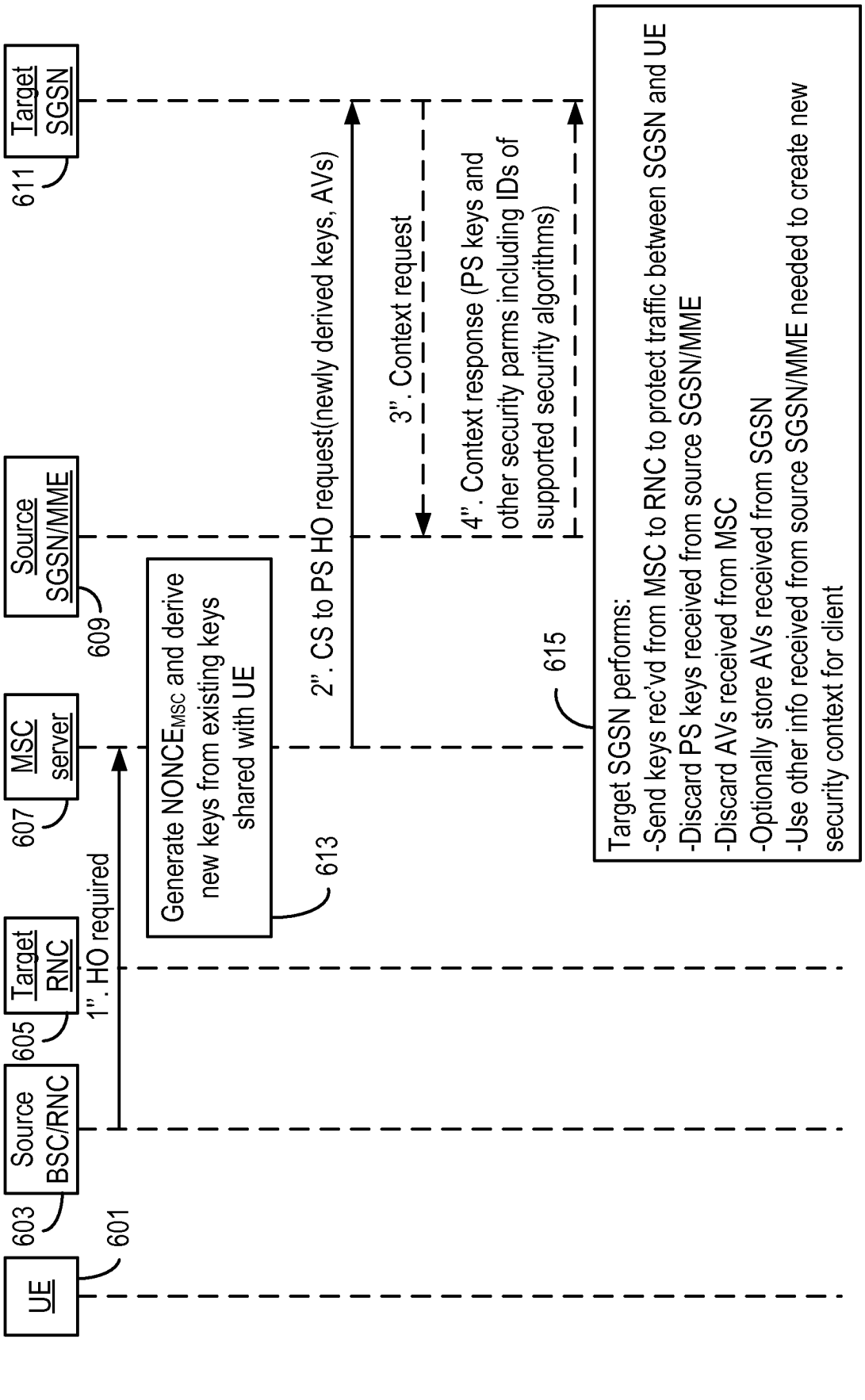
UE
601
Source BSC/RNC
603
Target RNC
605
MSC server
607
Source SGSN/MME
609
Target SGSN
611
1". HO required
Generate NONCE$_{MSC}$ and derive new keys from existing keys shared with UE
613
2". CS to PS HO request(newly derived keys, AVs)
3". Context request
4". Context response (PS keys and other security parms including IDs of supported security algorithms)
615
Target SGSN performs:
-Send keys rec'vd from MSC to RNC to protect traffic between SGSN and UE
-Discard PS keys received from source SGSN/MME
-Discard AVs received from MSC
-Optionally store AVs received from SGSN
-Use other info received from source SGSN/MME needed to create new security context for client
Steps 5, 6, 7, 8, 9, and 10 as shown in FIG. 3

FIG. 6

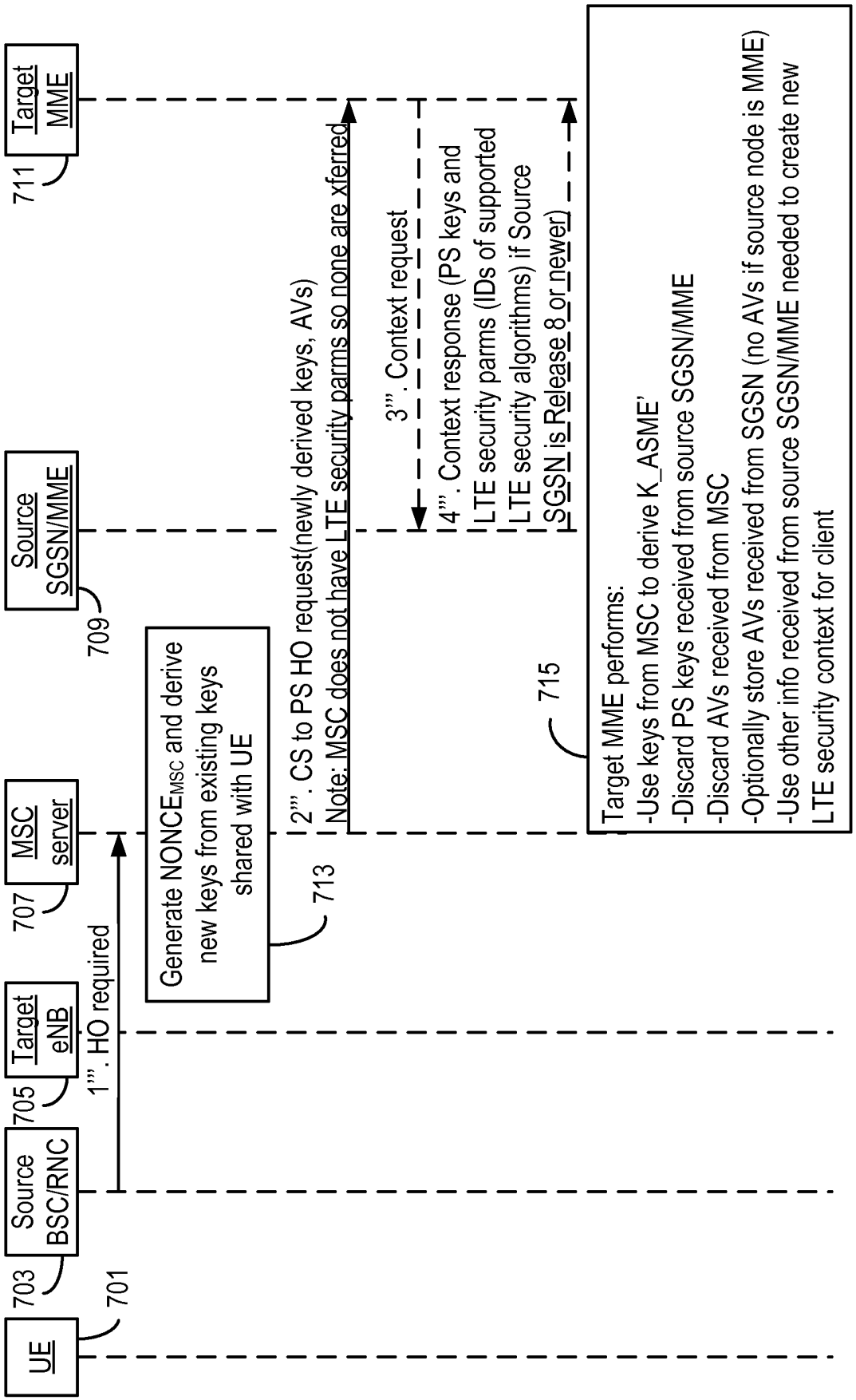
UE
701
Source BSC/RNC
703
Target eNB
705
MSC server
707
Source SGSN/MME
709
Target MME
711
1'''. HO required
Generate NONCE$_{MSC}$ and derive new keys from existing keys shared with UE
713
2'''. CS to PS HO request(newly derived keys, AVs)
Note: MSC does not have LTE security parms so none are xferred
3'''. Context request
4'''. Context response (PS keys and LTE security parms (IDs of supported LTE security algorithms) if Source SGSN is Release 8 or newer)
715
Target MME performs:
-Use keys from MSC to derive K_ASME'
-Discard PS keys received from source SGSN/MME
-Discard AVs received from MSC
-Optionally store AVs received from SGSN (no AVs if source node is MME)
-Use other info received from source SGSN/MME needed to create new LTE security context for client
Steps 5', 6', 7', 8', 9', and 10' as shown in FIG. 4

FIG. 7

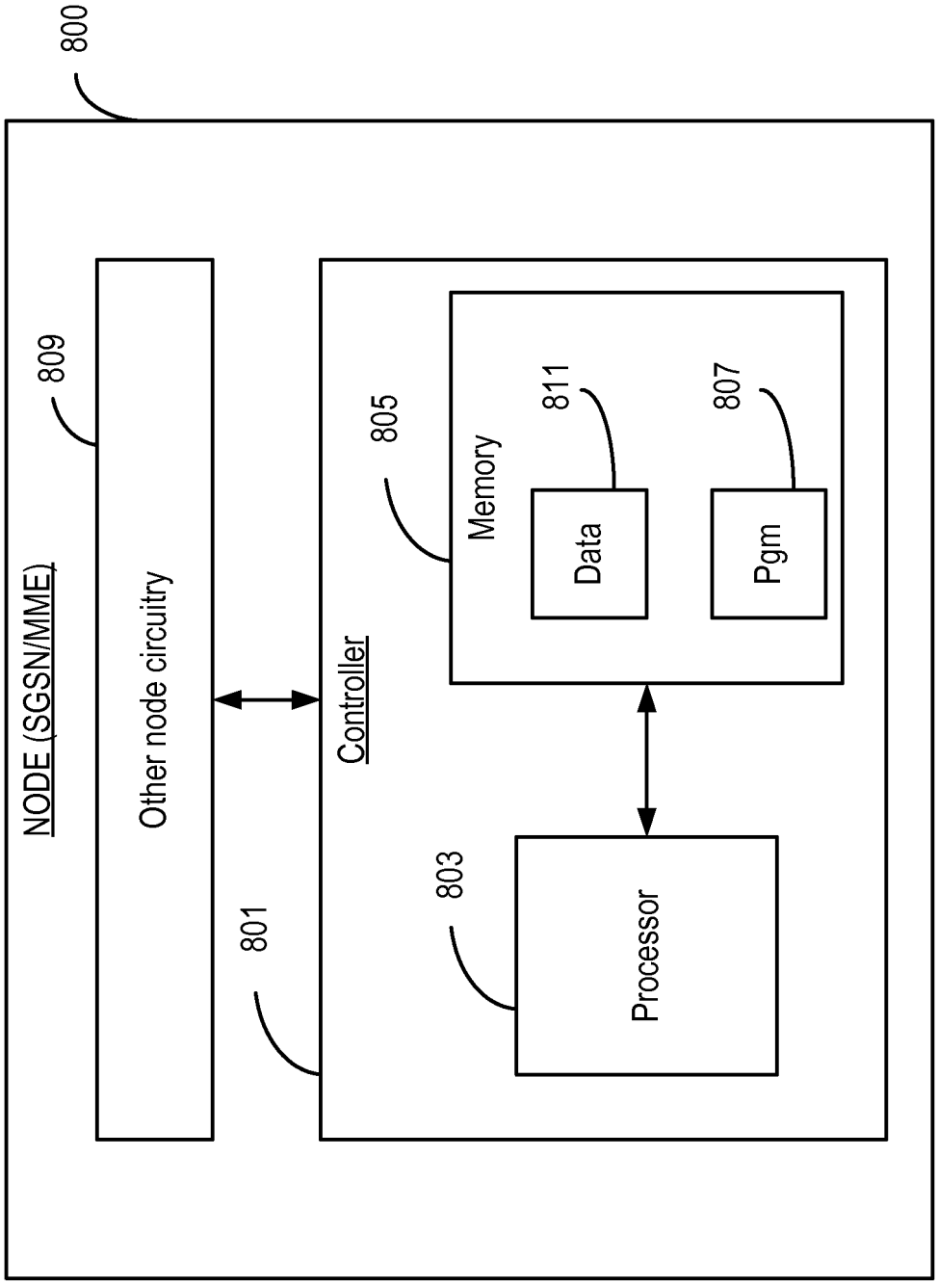
800
NODE (SGSN/MME)
809
Other node circuitry
801
Controller
805
Memory
811
Data
807
Pgm
803
Processor

FIG. 8

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Non-patent literature cited in the description

- *3GPP TS 23.060 V10.6.0,* December 2011 **[0020]**
- *3GPP TS 23.060* **[0020]**
- *3GPP TS 23.401 V10.6.0,* December 2011 **[0022]**